UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

STEPHANIE POTTS	)	**CLASS ACTION COMPLAINT**
	)	
v.	)	**CV-** 3:19-cv-01001 (DNH/ML)
	)	
CAPITAL ONE, N.A. and CAPITAL ONE FINANCIAL CORPORATION and CAPITAL ONE BANK (USA), N.A	)	

CLASS ACTION COMPLAINT

Plaintiff, through undersigned counsel, file on behalf of herself and all persons similarly situated, this Class Action Complaint, alleging the following based on personal knowledge, investigation of counsel and review of public documents. Among other things, as to allegations regarding the Plaintiff and on information and belief as to other allegations.

INTRODUCTION

1. This is a civil action seeking monetary damages, restitution and declaratory relief from Defendants Capital One Financial Corporation, Capital One, N.A. and Capital One Bank (USA), N.A (collectively, "Capital One"), arising from a data breach announced to the public on July 29, 2019.

2. From approximately March 12 to July 17 of 2019, the sensitive financial and personal data of an unknown number of customers was compromised as a result of Capital One's failure to adequately secure individual's personal and financial information on its systems.

3. Upon information and belief, during that period of time, an unauthorized person, identified as Paige Thompson of the State of Washington, intruded upon servers controlled by Capital One through a vendor of Capital One called Amazon Web Services, Inc. ("AWS"), a

division of Amazon, which provides cloud computing services to Capital One. Ms. Paige worked for AWS as a systems engineer from 2015 to 2016.

4. Ms. Thompson, who communicates online under the name "ERRATIC," was arrested on July 29, 2019 and is accused of the data breach by the FBI. *See U.S. v. Thompson*, Case No. MJ19-0344 (W.D. Wash.). She was able to intrude into Capital One's servers and exfiltrate customers' sensitive financial and personal data.

5. According to Capital One, 106 million people had their personal information stolen, including 100 million U.S. residents and 6 million Canadian residents who had, or applied for, Capital One accounts. The breach exposed 40,000 Social Security numbers and about 80,000 linked bank account numbers. The scope of the breach is massive. The bank says it became aware of it on July 19.

6. The information exposed included personal information like names, addresses, postal codes, phone numbers, email addresses, dates of birth and self-reported income. It also included credit scores, credit limits, balances, payment history, contact information and some transaction data from Capital One's systems.

7. Ms. Thompson took advantage of glaring weaknesses and vulnerabilities in the company's data security systems. Capital One's security protocols were so deficient the breach continued for over four months while Capital One failed to even detect it.

8. While Ms. Thompson was the perpetrator of the breach, its occurrence was inevitable. Capital One's systemic incompetence and a longstanding, lackluster approach to data security has existed within the company for years and is ingrained in its culture from the top down. Capital One's failure to seriously address data security persisted despite warnings by outside cybersecurity experts, the occurrence of other data breaches at Capital One and other numerous,

high-profile data breaches at other major American corporations, including Equifax, all of which should have alerted Capital One of the need to revamp and enhance its inadequate data security practices.

9. Plaintiff's Personal Information was exposed by Capital One. She seeks to recover damages and equitable relief on behalf of himself and all others similarly situated in the United States.

JURISDICTION AND VENUE

10. This Court has federal question subject-matter jurisdiction pursuant to 28 U.S.C. § 1331, because Plaintiff alleges that Capital One violated the FCRA.

11. In addition, this Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because (1) the Class consists of more than 100 members; (2) the amount at issue is more than $5 million exclusive of interest and costs; and (3) minimal diversity exists as at least one plaintiff is a citizen of a different state than Defendant.

12. This Court has jurisdiction over Capital One because the company regularly conducts business in Pennsylvania and has sufficient minimum contacts in Pennsylvania and Capital One, which has its principal headquarters in McLean, Virginia, has intentionally availed itself of this jurisdiction by marketing and selling products in Pennsylvania and to millions of consumers nationwide.

13. Venue in this Court is appropriate pursuant to 28 U.S.C. § 1391(a) because a substantial part of the events, acts, or omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

14. The Plaintiff identified below brings this action on behalf of herself and those similarly situated across the United States and within their State or Territory of residence. As with

the rest of the 100 million victims of the data breach, Capital One through its actions described herein leaked, disbursed, and furnished their valuable financial and personal information ("Personal Information")[1] to unknown cyber criminals, thus causing them present, immediate, imminent, and continuing increased risk of harm.

15. Plaintiff Stephanie Potts is a U.S. resident and citizen of the State of New York. Upon information and belief, her Personal Information was compromised in the data breach. Before the announcement of the breach, Plaintiff had a Capital One Platinum Mastercard for approximately eight months. She had also previously applied for an auto loan from Capital One. Capital One failed to safeguard the privacy and security of her information. Plaintiff would not have submitted her Personal Information had she known of Capital One's inadequate data security practices. Given the highly-sensitive nature of the information stolen, Plaintiff remains at a substantial and imminent risk of future harm.

16. Plaintiff is one of many individuals and businesses that have been impacted by the data breach.

17. Defendant Capital One Financial Corporation (COFC) is a Delaware corporation with its principal place of business in McLean, Virginia.

18. Defendant Capital One, N.A. (Cap One Bank) is a national bank incorporated in the State of Virginia with its principal place of business in McLean, Virginia. Cap One Bank is a wholly owned subsidiary of COFC.

---

[1] As defined herein and used throughout this Complaint, "Personal Information" includes all information exposed by the data breach, including but not limited to portions of a victim's name, address, postal code, phone numbers, email addresses, dates of birth, Social Security number, driver's license information tax identification number, bank account number, credit card number, personal images, income, credit scores, credit limits, account balances, payment history, and transaction data.

19. Defendant Capital One Bank (USA), N.A., (Cap One USA) is a national bank with its principal place of business in McLean, Virginia. Cap One USA is a wholly owned subsidiary of COFC.

20. Capital One regularly and systematically conducts business throughout the United States, including in this district. Among other things, Capital One is engaged in the business of providing loans, credit card services and retail banking services to millions of consumers, including Plaintiffs and members of the putative Classes. Capital One and its subsidiaries have an extensive branch network, with more than 900 branches, primarily in Connecticut, the District of Colombia, Maryland, Louisiana, New Jersey, New York, Texas, and Virginia. Capital One has been a national bank since March 1, 2008, subject to the National Bank Act, 12 U.S.C. § 1, *et seq.*, and regulations promulgated by the Office of the Comptroller of the Currency.

21. Capital One Chair and CEO Richard D. Fairbank said in a release: "While I am grateful that the perpetrator has been caught, I am deeply sorry for what has happened. I sincerely apologize for the understandable worry this incident must be causing those affected and I am committed to making it right."

CLASS ACTION ALLEGATIONS

22. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Fed. R. Civ. P. 23. This action satisfies the numerosity, commonality, typicality, adequacy, predominance and superiority requirements of Rule 23.

23. The proposed classes are defined as:

NATIONWIDE CLASS

> All natural persons and entities in the United States who, including individuals and businesses, within the applicable statute of limitations preceding the filing of this action to the date of class certification, whose Personal Information was compromised as a

> result of the data breach announced by Capital One on or about July 29, 2019.

24. The Nationwide Class asserts claims against Capital One for violation of the FCRA (Count 1), negligence (Count 2), and negligence misrepresentation (Count 3). The Nationwide Class also requests a declaratory judgment (Count 5).

25. Excluded from the Nationwide Class is Capital One and any of its parents, affiliates, or subsidiaries as well as any successors in interest or assigns of Capital One, the attorneys representing the class and the Judge assigned this litigation.

26. Upon information and belief, Plaintiff is a member of the Nationwide Class, as defined above.

STATEWIDE SUBCLASS

> All natural persons and entities in the State of New York who, including individuals and businesses, within the applicable statute of limitations preceding the filing of this action to the date of class certification, whose Personal Information was compromised as a result of the data breach announced by Capital One on or about July 29, 2019.

27. The members of the above Classes are readily ascertainable and Capital One likely has access to addresses and other contact information that may be used for providing notice to Class members.

28. The members of the Class are so numerous that joinder of all members would be impracticable. Plaintiffs are informed and believe—based upon Capital One's press releases — that there are approximately 100 million class members in the U.S. Those individuals' names and addresses are available from Capital One's records, and Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. There are also thousands of Class Members within each subclass.

29. There are substantial questions of law and fact common to the Classes that predominate over questions affecting only individual Class members including, but not limited to, the following:

a. Whether Capital One owed a duty to the Plaintiff and the Class to adequately protect Personal Information;

b. Whether Capital One breached its duty to protect Personal information by failing to provide adequate security;

c. Whether Capital One knew or should have known that its computer systems were vulnerable to attack;

d. Whether Capital One failed to take adequate and reasonable measures to ensure its data systems were protected;

e. Whether Capital One failed to take available steps to prevent and stop the breach from happening;

f. Whether Capital One's conduct (or lack thereof) was the direct and proximate cause of the breach of its systems, which resulted in the loss or disclosure of Personal Information;

g. Whether Capital One improperly retained transaction data beyond the period of time permitted by law;

h. Whether Capital One negligently failed to inform the Plaintiff and the Class regarding the vulnerabilities of its data protection systems, measures and practices;

i. Whether Capital One's conduct amounted to violations of the FCRA (15 USC §§ 1681, et seq.), state consumer protection statutes, and/or state data breach statutes

j. Whether the Plaintiff and the Class suffered financial injury as a result of Capital One's conduct (or lack thereof);

k. Whether the Plaintiff and the Class are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief; and

l. What is the appropriate measure of damages sustained by the Plaintiff and the Class?

30. Plaintiff's claims are typical of the Class. The same events and conduct that give rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class

member because Plaintiff has suffered harm as a direct and proximate cause of the same, specific data breach described herein.

31. Plaintiff will fairly and adequately represent the interests of the Class. Plaintiff has retained counsel who are experienced and qualified in prosecuting complex class action and data breach litigation similar to this one and Plaintiff intends to prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiff and his counsel. Neither Plaintiff nor their attorneys have any interest contrary to or conflicting with those of other members of the Class.

32. The prosecution of separate actions by individual Class members seeking declaratory and injunctive relief pursuant to Rule 23(b)(2) would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Capital One. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and impair their interests. Capital One has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

33. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the other Class members' claims is economically unfeasible and procedurally impracticable. Litigating the claims of the Class together will prevent varying, inconsistent, or contradictory judgments, and will prevent delay and unnecessary expense to the parties and the courts.

34. Even if Class members themselves could afford such individual litigation, the court system could not. Given the complex legal and factual issues involved, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized

litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a class action presents far fewer management difficulties, allows claims to be heard which might otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale and comprehensive supervision by a single court.

COMMON FACTUAL ALLEGATIONS

35. Capital One is one of the nation's top 10 largest banks based on deposits, with over 900 branch locations, thousands of ATMs, and online banking in eight states: Connecticut, Delaware, Louisiana, Maryland, New Jersey, New York, Texas and Virginia, and the District of Columbia. Capital One is in the business of providing its customers with a variety of banking and credit card services. Capital One offers credit cards and other services to customers throughout the United States. Capital One supports its services, in part, by renting or contracting for computer services provided by AWS for its cloud computing needs. The servers on which Capital One stores credit card application and other information generally store information regarding customers.

A. The Importance of Consumer Credit in the U.S. Economy

36. A consumer credit system allows consumers to borrow money or incur debt, and to defer repayment of that money over time. Access to credit enables consumers to buy goods or assets without having to pay for them in cash at the time of purchase.[2] Nearly all Americans rely on credit to make everyday purchases using credit cards, obtain student loans and further education, gain approval for items like cellular phones and Internet access, and to make major life purchases such as automobiles and homes.

---

[2] M. Greg Braswell and Elizabeth Chernow, Consumer Credit Law & Practice in the U.S., THE U.S. FEDERAL TRADE COMMISSION at 1, https://www.ftc.gov/sites/default/files/attachments/trainingmaterials/law_practice.pdf (last accessed July 30, 2019) ("FTC, Consumer Credit Law & Practice in the U.S.").

37. In order for this system of credit to be efficient and effective, a system of evaluating the credit of consumers is required. The earliest American systems of credit evaluation were retailers relying on personal reputation and standing in the community to determine creditworthiness. U.S. credit reporting agencies started as associations of retailers who shared their customers' credit information with each other including those deemed as credit risks.[3]

38. As the nation grew after World War II, and banks and finance companies took over from retailers as the primary source of consumer credit, a more quantitative and objective system of credit rating emerged. The development of computers, which could store and process large amounts of data, enabled banks like Capital One to efficiently share and review credit information on a national basis.[4]

39. A consumer's credit reporting file contains identifying information such as the consumer's name, date of birth, address, and Social Security Number, as well as payment information on past credit accounts, including the name of the lender, the original amount of the loan, the type of the loan, and how much money the consumer still owes on that loan. A consumer file also contains details on the consumer's payment history on past credit accounts—which helps potential lenders estimate how likely the consumer is to pay back the full amount of a loan on time—and information in the public record which might affect the consumer's ability to pay back a loan, such as recent bankruptcy filings, pending lawsuits, or information relating to tax liabilities.[5]

---

[3] *Id.*

[4] *Id.* at 2.

[5] *Id.* at 1.

40. Consumers have almost no control over the credit information gathered and stored about them. So the accuracy and security of the information is at the heart of a fair and accurate credit reporting system. Information that is inaccurate can lead to uninformed credit decisions, and information that is unsecure can lead to identify theft, fraud, and widespread distrust of the entities that store the data and the data itself, with systemic consequences for the entire national economy.

41. In March 1970, Alan Westin, a Columbia University professor, wrote an article in The New York Times that was critical of the all the information being collected to compile consumers' credit scores. When records went digital that same year, Congress reacted, enacting the FCRA in October 1970 "to promote the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies."

B. Capital One Discovers the Breach and the Hacker is Arrested

42. On July 17, 2019, Capital One received an anonymous email informing it that its data had been leaked. *See U.S. v Thompson*, ¶ 9.

43. Capital One examined the data file at issue, time-stamped April 21, 2019, and learned that it contained the IP address for a specific server. A firewall misconfiguration permitted commands to reach and be executed by that server. Code for commands within the file indicated that information held by AWS was extracted using an account with authenticated security credentials.

44. Capital One confirmed that the data extracted was its data and went back into its system and confirmed through logs that an intrusion had taken place allowing the user to extract the data on April 21, 2019.

45. By tracing the IP address of the user, Capital One was able to determine other intrusions undertaken by the same user. The intrusions began on March 12, 2019. Capital One reports that the data exfiltrated includes a large number of credit card applications – tens of millions potentially. According to Capital One, the data includes approximately 120,0000 Social Security Numbers and approximately 77,000 bank account numbers.

46. The FBI researched online activity on Twitter (username: ERRATIC) and a Meetup page. Based on the information reviewed and the information available in the April 21 file, the FBI has arrested Ms. Thompson and established problem cause to accuse her of intending to disseminate stolen data. The FBI then obtained a search warrant of MS. Thompson's residence and located additional information linking her to AWS, ERRATIC and the Capital One data breach.

C. Capital One Announces to the Data Breach to the World

47. On the evening of July 29. 2019, Capital issued a press release regarding the data breach.[6]

48. Capital One announced that "we believe it is unlikely that the information was used for fraud or disseminated by this individual."

49. Capital One stated that it "will make free credit monitoring and identity protection available to everyone affected." It estimated incremental costs as a result of the breach of approximately $100 to $150 million in 2019.

---

[6] *See* http://press.capitalone.com/phoenix.zhtml?c=251626&p=irol-newsArticle&ID=2405043 (last visited on July 30, 2019).

D. Capital One Understood the Value of Data Security

50. Like any bank or credit card issuer, Capital One was required to maintain the security and confidentiality of cardholder information and protect it from unauthorized disclosure.

51. The Payment Card Industry Data Security Standards ("PCI DSS") are a list of twelve information security requirements promulgated by the Payment Card Industry Security Standards Council. They apply to all organizations and environments where cardholder data is stored, processed, or transmitted and require organizations to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks and ensure the maintenance of information security policies. In addition, the PCI DSS prohibits Capital One from retaining certain customer data. Specifically, the PCI DSS 2.0 requires merchants to adhere to the following rules:

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored cardholder data
- Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security for all personnel

52. Capital One was at all times fully cognizant of its data protection obligations in light of the existing web of regulations requiring it to take affirmative steps to protect the sensitive

financial information entrusted to it by consumers and the institutions that participate in and administer payment card processing systems.

53. Despite this, Capital One's treatment of the sensitive Personal Information entrusted to it by its customers and the Plaintiff fell woefully short of its legal duties and obligations. Capital One failed to ensure that access to its data systems was reasonably guarded, protected from vendors, and failed to acknowledge numerous warning signs and properly utilize its own security systems that were put in place to detect and deter this exact type of attack. Capital One, at one point, even ***offered*** ID theft protection to its credit card customers.

54. At the time of the breach, Capital One had specific notice of the potential threat of a data breach, and of the potential risks posed to the Company and to the Plaintiff and the Class if Capital One failed to adequately protect its systems.

55. As early as 2005, a notorious IT systems hacker, Albert Gonzalez, masterminded and implemented one of the largest coordinated data breaches in history, ultimately compromising more than 170 million credit and debit card accounts by infecting retailers' point of sale ("POS") terminals with malicious software (also known as malware) which transmitted, unencrypted, the financial data being processed by the POS machine to Gonzalez and his accomplices. In the end, Gonzalez and his cohorts were able to walk off with vast amounts of customer data from various retailers.

56. Several noteworthy reports published in 2013 put. or should have put, all businesses on notice of the increase in cyber-attacks in the U.S. For instance, Visa Corporation issued reports alerting about specific attacks. To guard against the threat, Visa instructed companies to review its "firewall configuration and ensure only allowed ports, services and IP addresses are communicating with your network"; "segregate the payment processing network from other non-

payment processing networks"; "implement hardware-based point-to-point encryption"; "perform periodic scans on systems to identify storage of cardholder data and securely delete the data"; and "assign strong passwords to your security solution to prevent application modification." Capital One did not implement these measures.

57. Capital One's awareness of the importance of data security was bolstered in part by its observation of numerous other well-publicized data breaches involving major corporations being targeted for consumer information.

58. Through a series of data breaches extending back to 2013, more than three billion Yahoo user accounts were compromised when account holders' names, addresses, and dates of birth were stolen. The hackers also stole users' passwords, both encrypted and unencrypted, and security questions and answers.

59. In separate incidents in 2013 and 2014, hundreds of millions of retail customers were victimized by hacks of payment card systems at Target Stores and The Home Depot. Both breaches led to rampant payment card fraud and other damages both to consumers and to the card-issuing banks.

60. In the Summer of 2014, a data breach of JP Morgan Chase compromised the data of 76 million American households and 7 million small businesses. Breached data included contact information (names, addresses, phone numbers, and email addresses) as well as "internal information about the users."

61. In early 2015, Anthem, the second-largest health insurer in the United States, suffered a data breach that exposed the names, addresses, Social Security numbers, dates of birth, and employment histories of nearly 80 million current and former plan members.

62. Perhaps most significantly, data breaches to credit reporting agencies Experian, in 2015, exposing more than 15 million people's information, and Equifax, the largest breach yet, exposing more than half the countries' personal and financial information.

63. Unfortunately, Capital One did not view these breaches as cautionary tales, but rather as another avenue to profit from businesses and consumers concerned with fraud.

E. The Data Security Breach

64. In March of 2019, the Capital One data breach began.

65. Ms. Thompson was able to exploit glaring weaknesses in Capital One's systems by intruding upon servers controlled by a vendor of Capital One, AWS, a division of Amazon Inc. where Ms. Paige worked as a systems engineer from 2015 to 2016. AWS provides cloud computing services to Capital One. Other major data breaches were similarly exploited though access permitted by IT vendors.

66. Ms. Thompson used authenticated security credentials to gain access to the servers. Within the servers, there was a firewall misconfiguration that permitted commands to reach and be executed by that server. As a result, Ms. Thompson was able to enter Capital One's servers, execute commands, and remove customers' sensitive financial and personal data, all without being prevented from doing so, or even detected.

67. Capital One's security protocols were so deficient the breach continued for over four months while Capital One failed to even detect it. In fact, it took an anonymous tip for Capital One to learn that its data had been stolen.

68. Capital One's computer network was not properly protected to ensure its most sensitive parts were walled off from outsiders as well as the other parts of the network. Ms. Thompson did not take professional-level steps to exploit this gaping hole or hide her tracks – she

didn't have to. She was able to enter the most sensitive part of Capital One's computer system and exfiltrate million upon millions of private records. Security software exists that can detect these types of intrusions and prevent the removal of data, but Capital One's systems either did not contain such security software, the software was not running properly, or the IT professionals were not able to adequately use the software.

69. During this time, Capital One took no action to stop the attack. The data breach was preventable. Capital One could have blocked the intrusion by installing more rigorous security devices and being more diligent in its efforts to protect customer information.

70. Upon information and belief, information stolen from Capital One's systems quickly entered the black market.[7] Capital One's unreasonable data policies have cost the Plaintiff and the FI Class millions of dollars of damages.

71. Even though Capital One's recognizes the risk of failing to protect customers' personal information, it had not prioritized security: it was failing to adhere to industry standards regarding the retention and use of Personal Information, did not have adequate security on its systems to properly encrypt and/or tokenize information, did not have adequate anti-malware software, and did not have adequate security to otherwise protect against cyberattacks, and failed to properly update and maintain the security it had. Capital One further failed to adequately test and monitor its system for cyberattacks. These failures led to its vulnerability, but also may have put hackers like Ms. Thompson on notice this bank was cataloging and maintaining the Personal Information of its customers for the taking.

[7] The black market for personal and financial information is highly sophisticated, with numerous information-selling sites that are indistinguishable from a modern-day e-commerce site.

F. The Fallout Continues for Capital One Customers

72. The biggest threat is for people whose Social Security Number has been compromised. This number never changes.

73. Capital One's completely avoidable data breach inflicted significant financial damage upon the Plaintiff and the Class, who must act immediately to mitigate potentially present fraud, while simultaneously taking steps to prevent future fraud and while continuing to meet the demands and needs of their financial lives.

74. The costs suffered by the Plaintiff and the Class as a result of Capital One's data breach will continue to mount.

COUNT ONE
VIOLATION OF THE FAIR CREDIT REPORTING ACT, 15 U.S.C. §§ 1681, et seq.
(On Behalf of the Nationwide Class)

75. Plaintiff repeats and realleges Paragraphs 1-74 as if fully alleged herein.

76. Each time that Capital One opens or potentially opens a new account or starts a new financial service, it obtains, reviews, and use a "consumer report," as that term is defined in 15 U.S.C § 1681a(d), about the person or entity for whom the account is opened or the service started.

77. Capital One is required by 15 U.S.C. §§ 1681b, 1681n, and 1681o to refrain from obtaining, disclosing or using consumer reports under false pretenses, and without proper authorization from the person or entity who is the subject of the report.

78. The furnishing of a consumer report is only permitted in specific instances. 15 U.S.C. §§ 1681b(a). Disclosing, or allowing consumer reports to be disclosed, is not allowed pursuant to FCRA, and thus is a violation of federal law.

79. Once obtained, Capital One has a mandatory duty to maintain and protect the use of consumer reports for permissible purposes only. 15 U.S.C. § 1681b(f). That includes instances

where, but for actions taken or not taken by Capital One in data protection, the use of unlawful consumer reports obtained would not have occurred.

80. Despite these clear and unambiguous requirements of the FCRA, Capital One's actions and inactions has caused and will cause consumer reports regarding consumers to be obtained without their knowledge or consent in order to potentially open new, unauthorized accounts and services, in violation of FCRA.

81. Further, reports that were obtained in relation to the applications for credit were part of the collection of data that was exfiltrated in the data breach. Accordingly, Capital One failed to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

82. Capital One failed to maintain reasonable procedures designed to limit the furnishing of Class members' consumer reports to permitted purposes, and/or failed to take adequate security measures that would prevent disclosure of Class members' consumer reports to unauthorized entities or computer hackers.

83. As a direct and proximate result of Capital One's actions and failures to act described herein, and utter failure to take adequate and reasonable measures to ensure its data systems were protected, Capital One offered, provided, and furnished Plaintiff's and Class members' consumer reports to unauthorized third parties.

84. Pursuant to 15 U.S.C. §§ 1681n and 1681o, Capital One is liable for negligently and willfully violating FCRA by accessing the consumer reports without a permissible purpose or authorization under FCRA.

COUNT TWO
NEGLIGENCE
(On Behalf of the Nationwide Class)

85. Plaintiff repeats and realleges Paragraphs 1-84 as if fully alleged herein.

86. Capital One owed a duty to the Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, securing, and deleting the Personal Information of customers.

87. Capital One owed a duty to Plaintiffs and the Class to provide security, consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the Personal Information of customers.

88. Capital One owed a duty of care to the Plaintiff and the Class because they were a foreseeable and probable victim of any inadequate data security practices. Capital One solicited, gathered, and stored the sensitive data provided by the Plaintiff and the Class. Capital One knew it inadequately safeguarded this information on its computer systems and that hackers would attempt to access this valuable data without authorization. Capital One knew that a breach of its systems would inflict millions of dollars of damages upon the Class, and Capital One was therefore charged with a duty to adequately protect this critically sensitive information.

89. Capital One maintained a special relationship with the Class. The Class entrusted Capital One with Personal Information on the premise that it would safeguard this information, and Capital One was in a position to protect against the harm suffered by the Class as a result of the data security breach.

90. In light of its special relationship, Capital One knew, or should have known, of the risks inherent in collecting and storing the sensitive information and the importance of providing adequate security of that information.

91. Capital One's own conduct also created a foreseeable risk of harm. Its misconduct included, but was not limited to, it not following broadly accepted security practices and not complying with industry standards for the safekeeping and maintenance of Personal Information.

92. Capital One breached the duties it owed by failing to exercise reasonable care and implement adequate security protocols—including protocols required by industry rules—sufficient to protect the Personal Information at issue.

93. Capital One breached the duties it owed by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

94. Capital One breached the duties it owed by failing to properly maintain the sensitive Personal Information. Given the risk involved and the amount of data at issue, Capital One's breach of its duty was entirely unreasonable.

95. Capital One also knew that the Plaintiff and the Class were foreseeable victims of a data breach of its systems because of specific laws, regulations, and guidelines requiring it to reasonably safeguard sensitive information or be held liable in the event of a data breach.

96. As a direct and proximate result of Capital One's negligent conduct, the Plaintiff and the Class has suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT THREE
NEGLIGENT MISREPRESENTATION
(On Behalf of the Nationwide Class)

97. Plaintiff repeats and realleges Paragraphs 1-96 as if fully alleged herein.

98. Through its privacy policies and other actions and representations, Capital One misrepresented to the Plaintiff and the Class that it possessed and maintained adequate data security measures and systems that were sufficient to protect Personal Information.

99. Capital One further misrepresented that it would secure and protect Personal Information by agreeing to comply with both Card Operating Regulations and the PCI DSS.

100. Capital One knew or should have known that it was not in compliance with the representations made in its privacy policies and the requirements of Card Operating Regulations and the PCI DSS.

101. Capital One knowingly and deliberately failed to disclose material weaknesses in its data security systems and procedures that good faith and common decency required it to disclose to the Plaintiff and the Class.

102. A reasonable business would have disclosed information concerning material weaknesses in its data security measures and systems to the Plaintiff and the Class.

103. Capital One also failed to exercise reasonable care when it failed to timely communicate information concerning the data breach that it knew, or should have known, compromised the Personal Information of customers.

104. Plaintiff and the Class relied upon these misrepresentations and omission to their detriment.

105. As a direct and proximate result of Capital One's negligent misrepresentations by omission, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT FOUR
VIOLATIONS OF NEW YORK BUSINESS LAW
(On Behalf of the State Subclass)

106. Plaintiff repeats and realleges Paragraphs 1-105 as if fully alleged herein.

107. This claim is asserted on behalf of the members of the State Subclass under New York's Consumer Protection Law. Gen. Bus. Law 349 *et seq* ("GBL").

108. Plaintiff and Defendants are "persons" under New York General Business Law § 349(h), and Defendants' conduct occurred in the course of trade or commerce.

109. Defendants' conduct constitutes prohibited "[d]eceptive acts or practices in the conduct of any business, trade, or commerce," N.Y. Gen. Bus. Law § 349.

110. Capital One's collection of Personal Information for financial accounts constitutes unfair competition or unfair or deceptive acts or practices in violation of the GBL.

111. Capital One's actions set forth herein also violate including but not limited to GBL § 350 for false advertising. Capital One advertises its services, in particular, its banking, credit card and loan services, as secure from third party eyes, including protected from hackers' exfiltration and sale of consumers' Personal Information. In failing to protect, consumers' Personal Information, and in failing to maintain systems that are capable of doing so, Capital One has engaged in false advertising.

112. Capital One engaged in unlawful conduct, made affirmative misrepresentations, or otherwise violated the UTPCPL by, *inter alia*, knowingly and intentionally collecting and failing to adequately protect Personal Information, and misrepresenting and failing to disclose its inadequate policy and practice of protecting Personal Information.

113. Capital One also engaged in unlawful conduct in violation of the UTPCPL by making knowing and intentional omissions. Capital One knowingly failed to disclose the true nature of its data security policy and practice.

114. Capital One intended that Plaintiff and all Class Members rely on the acts of concealment and omissions, so that Plaintiff and all Class Members would feel secure providing Capital One their valuable Personal Information.

115. Capital One's conduct caused Plaintiff and Class members to suffer actual, ascertainable losses that, but for Capital One's unfair and deceptive policy, would not otherwise have been incurred.

116. Under GBL § 349 (h), Plaintiff and the other members of the Class are entitled to recover actual damages or fifty dollars for herself and all the other Class members, whichever is greater, or both such actions. The Court may, in its discretion, increase the award of damages to an amount not to exceed three times the actual damages up to one thousand dollars, if the Court finds the defendant willfully or knowingly violated this section. The Court may award reasonable attorney's fees to a prevailing plaintiff.

117. A causal relationship exists between Capital One's unlawful conduct and the ascertainable losses suffered by Plaintiff and the Class. Had Capital One adequately protected the Personal Information at issue here, Plaintiff and the Class would not have incurred losses in violation of the UTPCPL.

118. As redress for Capital One's repeated and ongoing violations of the UTPCPL, Plaintiff and the State Subclass are entitled to, *inter alia*, damages, declaratory relief and injunctive relief.

119. The Court should declare Capital One's practices to be unlawful, unfair, unconscionable and/or deceptive, and enjoining Capital One from undertaking any further unlawful, unfair, unconscionable, and/or deceptive acts or omissions.

120. Because Plaintiff seeks to enforce an important right affecting the public interest, Plaintiff requests an award of attorneys' fees and costs on behalf of herself and the Class.

COUNT FIVE
DECLARATORY RELIEF
(On Behalf of the Nationwide Class and the State Subclass)

121. Plaintiff repeats and realleges Paragraphs 1-120 as if fully alleged herein.

122. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant

further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

123. An actual controversy has arisen in the wake of the Capital One data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Capital One is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their Personal Information. Plaintiff allege that Capital One's data security measures remain inadequate. Capital One denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future.

124. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Capital One continues to owe a legal duty to secure consumers' Personal Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Capital One continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Personal Information.

125. The Court also should issue corresponding prospective injunctive relief requiring Capital One to employ adequate security protocols consistent with law and industry standards to protect consumers' Personal Information.

126. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Capital One. The risk of another such breach is real, immediate, and substantial. If another breach at Capital One occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

127. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Capital One if an injunction is issued. Among other things, if another massive data breach occurs at Capital One, Plaintiff will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Capital One of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Capital One has a pre-existing legal obligation to employ such measures.

128. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Capital One, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of himself and the Class, respectfully requests that the Court enter judgment in their favor as follows:

a. certifying the Class under Fed. R. Civ. P. 23 and appointing Plaintiff and its counsel to represent the Class pursuant to Fed. R. Civ. P. 23(g);

b. awarding Plaintiff and the Class monetary damages as allowable by law;

c. awarding Plaintiff and the Class appropriate equitable relief;

d. awarding Plaintiff and the Class pre-judgment and post judgment interest;

e. awarding Plaintiff and the Class reasonable attorneys' fees and costs as allowable by law; and

f. awarding all such further relief as allowable by law.

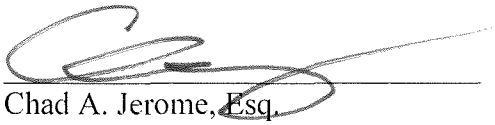
JURY TRIAL DEMANDED

Plaintiff, on behalf of herself and the Class, demands a trial by jury on all issues so triable.

Richard M. Golomb, Esquire
Kenneth J. Grunfeld, Esquire
GOLOMB & HONIK, P.C.
1835 Market Street, Suite 2900
Philadelphia, PA 19103
Phone: (215) 985-9177
Fax: (215) 985-4169

Attorneys for Plaintiff and the Class

O'CONNELL & ARONOWITZ, P.C.

By: 

Chad A. Jerome, Esq.
Of Counsel to Golomb & Honik, P.C.
Bar Roll #: 514348
54 State Street, 9th Floor
Albany, New York 12207
Phone: (518) 462-5601
Fax: (518) 462-2670

Dated: August 13, 2019